IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR DEVICE ASSIGNED CALL NUMBER (207) 576-7593, THAT IS STORED AT PREMISES CONTROLLED BY VERIZON	Case No. 21-mj-272-AJ-01 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF

AN APPLICATION FOR A SEARCH WARRANT

I, Adam Rayho, a Task Force Officer with Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number (207) 576-7593, ("the SUBJECT PHONE"), that is stored at premises controlled by Verizon, a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey 07921. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Verizon to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I

of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a detective with the Nashua, New Hampshire Police Department, and a deputized task force officer (TFO) for HSI. I became a certified police officer in the State of New Hampshire in May 2014 after graduating from the 164th New Hampshire Police Standards and Training Academy. I have also completed HSI's Task Force Officer Course. I hold a bachelor's degree in criminal justice, with a minor in Computer Science and Victimology, from Endicott College.

3. Since November 2019, I have been assigned to the Special Investigations Division as a member to the New Hampshire Internet Crimes Against Children (ICAC) Task Force, which includes numerous federal, state, and local law enforcement agencies conducting proactive and reactive investigations involving online child exploitation. As a TFO, I am authorized to investigate violations of federal laws and to execute warrants issued under the authority of the United States. Specifically, as a TFO and a member of the ICAC, I investigate criminal violations related to online sexual exploitation of children. I have received training in the areas of child sexual exploitation including, but not limited to, possession, distribution, receipt, and production of child pornography, and interstate travel with intent to engage in criminal sexual activity, by attending training hosted by the ICAC involving online undercover chat investigations and interview/interrogation. I have also participated in numerous online trainings hosted by the Federal Bureau of Investigation Child Exploitation and Human Trafficking Task Force Online Covert Employee Development Series. These trainings focused on live stream investigations and using undercover personas on various social media applications for proactive investigations. I have personally conducted numerous online undercover investigations using

social media applications such as KIK messenger, Grindr, WhatsApp, Whisper, and MeetMe. In addition, I have completed the Cellebrite Certified Operator and Cellebrite Certified Physical Analyst course in mobile forensics. Furthermore, I have completed trainings offered by the Internet Crimes Against Children Task Force, National Training Program which is a program of the Fox Valley Technical College – National Criminal Justice Training Center, on BitTorrent investigations, to include the BitTorrent Overview, ICAC BitTorrent Update and Refresher, Corroborating BitTorrent Investigations, and interview techniques in P2P Investigations. In the course of investigating crimes related to the sexual exploitation of children, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous online child sexual exploitation investigations and am very familiar with the tactics used by child pornography offenders who collect child pornographic material and those who seek to exploit children.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that a violation of 18 U.S.C. § 2252A(a)(2) has been committed using the SUBJECT PHONE. There is also probable cause to search the information described in Attachment A for evidence of this crime as further described in Attachment B.

BACKGROUND ON PEER-TO-PEER SOFTWARE

6. A significant aspect of the Internet is peer-to-peer, or P2P. P2P file-sharing is a method of communication available to Internet users through the use of special software such as

BitTorrent. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the information is first deposited before it is distributed. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from one folder to another to stop the distribution across the Internet. Further, once a file or files are placed in a shared folder its distribution is dependent only on the machine being turned on and connected to the Internet.

7. BitTorrent is one type of P2P file-sharing software. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts or the actual file(s) being sought. The download of

the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

8. One of the advantages of P2P file-sharing is that multiple files may be downloaded at the same time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading a movie file may actually receive parts of the movie from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. It is possible to also download the file or files from only one computer.

9. The BitTorrent Network bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the digital fingerprinting of data. Once you check a file or files with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

PROBABLE CAUSE

10. During the month of August 2021 Detective Peter LaRoche (NPD) and I initiated a proactive online investigation on the peer-to-peer [P2P] sharing software known as BitTorrent. This investigation focused on users sharing child sexual abuse material on the BitTorrent Network. The software used by law enforcement identifies shared files that other investigations have determined may contain child pornography and / or related material, and automatically tries to download them

11. While reviewing downloads using the BitTorrent software, Detective LaRoche and I were able to identify a natting IP address[1] which was being utilized to share child sexual abuse material ("CSAM") on several dates in late August 2021 and early September 2021. The Torrent being shared is identified as:

Torrent info hash (hexadecimal): 0e3615ebad8fdb594653a995f25d588f2d347d62

Number of files defined by the torrent: 5782

12. The BitTorrent software identified the IP address, port number, date, and time in which the user was sharing the torrent with the UC BitTorrent software as:

-IP address 174.255.66.236 port 6320 on 08-31-2021 at 18:12:39 UTC

Status: Terminated

Files: 5782

Completed: 3631

-IP address 174.255.66.56 port 13060 on 08-31-2021 at 18:21:12 UTC

Status: Terminated

Files: 5782

Completed: 5763

-IP address 174.255.66.104 port 1514 on 08-31-2021 at 21:26:43 UTC

Status: Terminated

[1] A natting IP address is an IP address in which multiple users have access to, but are uniquely identified through their telephone number

Files: 5782

Completed: 5535

-IP address 174.255.68.75 port 14719 on 09-01-2021 at 13:56:45 UTC

Status: Terminated

Files: 5782

Completed: 5570

-IP address 174.255.67.135 port 26701 on 09-01-2021 at 20:53:47 UTC

Status: Terminated

Files: 5782

Completed: 5763

-IP address 174.255.66.66 port 19769 on 09-02-2021 at 15:32:46 UTC

Status: Terminated

Files: 5782

Completed: 1427

-IP address 174.255.68.13 port 3055 on 09-02-2021 at 15:19:37 UTC

Status: Terminated

Files: 5782

Completed: 5763

-IP address 174.255.68.220 port 22334 on 09-03-2021 at 15:04:57 UTC

Status: Terminated

Files: 5782

Completed: 5762

-IP address 174.255.65.49 port 5260 on 09-03-2021 at 17:46:08 UTC

Status: Terminated

Files: 5782

Completed: 5763

-IP address 174.255.67.214 port 21718 on 09-04-2021 at 15:08:24 UTC

Status: Terminated

Files: 5782

Completed: 5763

-IP address 174.255.67.237 port 8282 on 09-04-2021 at 18:01:33 UTC

Status: Terminated

Files: 5782

Completed: 4269

-IP address 174.255.66.191 port 12665 on 09-05-2021 at 16:01:20 UTC

Status: Terminated

Files: 5782

Completed: 5654

-IP address 174.255.65.148 port 11329 on 09-05-2021 at 18:34:10 UTC

Status: Terminated

Files: 5782

Completed: 2665

-IP address 174.255.68.44 port 10890 on 09-07-2021 at 12:10:27 UTC

Status: Terminated

Files: 5782

Completed: 5763

-IP address 174.255.68.186 port 2634 on 09-08-2021 at 19:31:53 UTC

Status: Terminated

Files: 5782

Completed: 5763

-IP address 174.255.67.78 port 19249 on 09-10-2021 at 00:20:11 UTC

Status: Terminated

Files: 5782

Completed: 5763

-IP address 174.255.64.141 port 1575 on 09-10-2021 at 01:31:22 UTC

Status: Terminated

Files: 5782

Completed: 5763

13. Upon reviewing each connection, I observed the status was listed as "terminated". This regularly occurs during undercover BitTorrent investigations as the software is primarily designed for users to receive and share files, which the law enforcement software does not do.

The software used by law enforcement only receives files of investigative interest; thus, the sessions regularly terminate without completing the full download.

14. During each connection, the software received varying amounts of the torrent from the SUBJECT PHONE. In total, the torrent contained 5,782 files. The most that the SUBJECT PHONE shared during a session was 5,763 files, which occurred on nine occasions, as listed above.

15. I reviewed the files which were received from the SUBJECT PHONE and observed that, during the sessions in which 5,763 files were received, the files were all contained under a main folder titled "awe pthc[2] videos." The "awe pthc videos" folder contained several subfolders which contained CSAM, the large majority of which depicts prepubescent and toddler children.

16. Specifically, in the "My Babygirls(2Yo Suck Fuck)" subfolder were 45 images which depicted a prepubescent female toddler. Two of the files within this folder which qualified as CSAM are described as:

Filename: 2yo-0058
Description: digital image of a prepubescent female toddler. The toddler is lying on her back with her legs up in the air/spread and is naked. An adult's hands are spreading the female's vaginal opening, which is the focal point of the image. In identifying the female depicted in the image as prepubescent, I base this conclusion on her body structure, physical features, and lack of pubic hair.

[2] "PTHC" is a common phrase used in child exploitation which stands for "pre-teen, hard core".

Filename: janet-008F

Description: digital image of a prepubescent female toddler and an adult male. The image captures the area of the toddler's vaginal opening, which has a male's genitalia pressed up against it. In identifying the female depicted in the image as prepubescent, I base this conclusion on her body structure, physical features, and lack of pubic hair.

17. Specifically, in the "black tod" sub folder was another subfolder titled "black toddler" which contained two files. The two files both qualified as CSAM are described as:

Filename: 1171516240476.jpg

Description: digital image of a prepubescent female lying on her stomach. The female is completely naked and the angle from which the image is taken makes the focal point the female's vaginal and anal openings. In identifying the female depicted in the image as prepubescent, I base this conclusion on her body structure, physical features, and lack of pubic hair.

Filename: img20060910193712.jpg

Description: digital image of a prepubescent female and an adult male. The male has his erect penis exposed and the female is in close proximity with her mouth open. In identifying the female depicted in the image as prepubescent, I base this conclusion on her body structure and physical features.

18. The titles of the additional sub folders which contained CSAM are:

"!!! NEW 616 babypics – mixed&sorted"

"%283-sisters%29"

“4_sungl”

“4y_assfk”

“2008 pics Megan”

“ashley”

“dd”

“falko”

“Katie Kbaby pthc”

“Liseth [5yo]

“Photos (4yo bride)”

“Scargirl’s Lil Sis”

“Toddler PTHC extremely 0 – 10yo 2008”

“My Babygirls(2Yo Suck Fuck)”

“black tod”

19. I searched the aforementioned IP addresses using the American Registry of Internet Numbers (ARIN) and learned each IP address belonged to Verizon.

20. On September 06, 2021 I completed a summons to obtain subscriber information for the aforementioned IP addresses. The summons was served to Verizon and I later received the results which showed each IP address was associated with the telephone number 207-576-7593.

Verizon identified this phone number as utilizing their cell phone towers but belonging to Tracfone Wireless Inc.

21. On October 01, 2021 I completed a summons to obtain subscriber information from Tracfone for the telephone number 207-576-7593. The results of this summons are still pending.

22. Using various open source research databases, I researched the phone number 207-576-7593 but could not identify any individuals associated with the number.

23. In my training and experience, I have learned that Verizon is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

24. Based on my training and experience, I know that Verizon can collect cell-site data about the SUBJECT PHONE. I also know that wireless providers such as Verizon typically collect and

retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

25. Based on my training and experience, I know that Verizon also collects per-call measurement data, which Verizon also refers to as the "real-time tool" ("RTT"). RTT data estimates the approximate distance of the cellular device from a cellular tower based on the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

26. Based on my training and experience, I know that wireless providers such as Verizon typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as Verizon typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT PHONE's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

27. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

28. I further request that the Court direct Verizon to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or

control. Because the warrant will be served on Verizon, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Adam Rayho
Adam Rayho
Task Force Officer
Homeland Security Investigations

Subscribed and sworn to before me on October 14, 2021

Honorable Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number 207-576-7593 ("the Account"), that is stored at premises controlled by Verizon ("the Provider"), a wireless telephone service provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey 07921.

ATTACHMENT B

Particular Things to be Seized

Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period of August 30, 2021 at 00:00:00 UTC through September 11, 2021 at 00:00:00 UTC:

a. The following information about the customers or subscribers of the Account:

i. Names (including subscriber names, user names, and screen names)

ii. Addresses (including mailing addresses, residential addresses, business addresses and email addresses)

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"),

Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received

ii. Per Call Measurement Data (PCMD) data (also known as the "real-time tool" or "RTT" data)

Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband and instrumentalities of a violation of 18 U.S.C. § 2252A(a)(2) involving the SUBJECT PHONE from August 30, 2021 to September 11, 2021.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the

government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Verizon, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Verizon. The attached records consist of the following type of records: _____. I further state that:

a) all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Verizon, and they were made by Verizon as a regular practice; and

b) such records were generated by Verizon's electronic process or system that produces an accurate result, to wit:

    1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Verizon in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Verizon, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature